11/appeal Brief

Attorney Docket No.: 50325-0080

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Jonathan TROSTLE, et al.) Confirmation No.

Serial No.: 09/482,156) Examiner: Khanh Dinh

Filing Date: January 12, 2000) Art Unit: 2172

For: DIRECTORY ENABLED SECURE MULTICAST GROUP COMMUNICATIONS)

BOX AF
Commissioner for Patents
Washington, D.C. 20231

APPEAL BRIEF

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed November 19, 2002.

I. REAL PARTY IN INTEREST

Cisco Systems, Inc.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

In paragraph 5, the Office Action rejected Claims 1–9 under 35 U.S.C 103(a) as allegedly unpatentable over U.S. Patent No. 6,240,188B1 issued to Dondeti, et al. on May 29, 2001, *(Dondeti)* in view of U.S. Patent No. 6,279,112B1 issued to O'Toole, Jr. et al. on August 21, 2001 (*O'Toole*).

In paragraph 8, the Office Action rejected Claims 10-18 under 35 U.S.C. 103(a) as allegedly unpatentable over *Dondeti* in view of *O'Toole.*

In paragraph 11, the Office Action rejected Claims 19-25 under 35 U.S.C. 103(a) as allegedly unpatentable over *Dondeti* in view of *O'Toole.*

IV. STATUS OF AMENDMENTS

No amendments to the specification or the claims have been made after the final reply to the first Office Action dated November 8, 2002.

V. SUMMARY OF THE INVENTION

The invention provides a significant advance in achieving scalable secure communication within multicast groups of network devices such as routers, switches and gateways. To provide secure communication, multicast group members encrypt messages sent within the group. The invention addresses how to efficiently generate and distribute encryption keys to group members.

As explained in the application as filed, many contemporary cryptography approaches use key-based algorithms. Generally, two types of key-based algorithms exist: symmetric algorithms and asymmetric algorithms, of which one example is a public key algorithm. As a practical matter, a "key" forms one of the inputs to a mathematical function that is used by a computer or processor to generate a ciphertext.

Public key algorithms are designed so that the key used for encryption is different than the key used for decryption. The decryption key cannot be determined from the encryption key, at least not in any reasonable amount of time with practical computing resources. Typically, the encryption key (public key) is made public so that anyone, including an eavesdropper, can use the public key to encrypt a message. However, only a specific participant in possession of the decryption key (private key) can decrypt the message.

Public key algorithms, however, often are not employed as a mechanism to encrypt messages, largely because such algorithms consume an inordinate amount of system resources and time to encrypt entire messages. As a result, a public key cryptosystem is utilized only to establish a secure data communication channel through key exchanges among the participants. That is, two or more parties, who wish to communicate over a secure channel, exchange or make available to each other public (or non-secure) key values. In the Diffie-Hellman algorithm, each party uses the other party's public key value to privately and securely compute a secret key, using an agreed upon algorithm. The parties then use their derived secret keys in a separate (often symmetric) encryption algorithm to encrypt messages passed over the data communication channel. Conventionally, these secret keys are valid only on a per communication session basis, and thus are referred to as session keys. These session keys can be sued to encrypt/decrypt a specified number of messages or for a specified period of time.

When a multicast group is established, management of the session's keys due to membership changes poses a number of problems. Forward secrecy, which arises when a member node leaves the multicast group and may still possess the capability to decipher future messages exchanged among the group, becomes a concern. In addition, when a new member node enters the multicast group, the new member should not be permitted to decrypt the past messages of the multicast group. Session key updates when a "join" or "leave" occurs need to be performed rapidly to avoid undue system delay. This issue relates to how well the network scales to accommodate additional users.

In the applicants' specification, FIG. 1 is a block diagram of one approach to establish secure communication that employs a key distribution center (KDC) to regulate the exchange of keys. A single central group controller (GC) 1001 is responsible for distributing, creating, and updating session keys to the members of the multicast group comprising users A-H. The users A-H communicate with the group controller 1001 via separate point-to-point connections 1003 to obtain the dynamic group session key. Channels 1003 can be made secure by using a standard Diffie-Hellman key exchange protocol in which nodes A-H exchange with the centralized group controller.

A drawback is that the group controller 1001 is a potential bottleneck in the network. For instance, if multiple nodes request to join the multicast group, the group controller may not be able to process such requests in a timely manner. This problem is especially pronounced if the multicast group is distributed over a wide area network (WAN). Further, the group controller 1001 does not scale well, due in part to physical hardware constraints. In addition, each node A-H and the group controller must have specialized software for creating and processing messages. It would be an advance if a general-purpose infrastructure software layer could perform key distribution.

According to one aspect of the invention, a method is provided for creating a plurality of secure multicast groups. The method involves, in one embodiment, creating event types in a multi-master directory. Events are defined as multicasted messages. Publishers are network entities such as routers and switches that send events to other network entities in the role of subscribers who receive events. The multi-master directory provides access controls for individual objects and attributes. The subscribers and publishers are authenticated, and each of the subscribers and publishers has a secret key. The subscribers and publishers access the directory to determine events that they may process.

The method further includes registering the subscribers and the publishers with an event server. As detailed in Applicants' reply of August 14, 2002 and the accompanying references, event servers generally are message handling infrastructure elements that use a publish-subscribe metaphor and are quite different from group controllers. The event server determines whether the publishers are authorized to produce certain events corresponding to the event types and whether the subscribers are authorized to receive certain events. If so, a group session key is generated for establishing one of the multicast groups. The group session key is encrypted in a message that has a prescribed format. The subscribers receive the message. Additionally, the method includes determining whether the received message corresponds to a correct key version, updating the group session key by the event server, and selectively reregistering the subscribers. An event server is co-located with each directory service.

Other embodiments and aspects provide a communication system for creating a plurality of secure multicast groups, and a computer system for establishing multiple secure multicast groups. Each of these embodiments and aspects involves use of an event for selectively generating a group session key and private keys corresponding to the plurality of principals, and for distributing keys. These systems leverage a scalable network of event servers for creating multicast secure communication channels.

Still other embodiments provide for key changes by initiating a key change event from a master event server, and using a change password protocol to generate the new key. As described in the specification at page 19, the key change event includes the new key in an event type object of the key change event, which is multicast to the nodes. Thus, an event server is efficiently used to distribute new keys to nodes participating in a multicast group.

By integrating an event server, network nodes in multicast groups and a replicated multi-master directory with per object and per attribute access controls, the invention provides scalability on a level that otherwise cannot be achieved. Use of an event server provides key distribution and management through an infrastructure layer that is adapted for an entirely new purpose. The event "bus" handles all message communication details so that no special group controller message protocol is needed.

VI. ISSUES

Whether Claims 1-9 are patentable under 35 U.S.C 103(a) as nonobvious over *Dondeti* in view of *O'Toole.*

Whether Claims 10-18 are patentable under 35 U.S.C 103(a) as nonobvious over *Dondeti* in view of *O'Toole.*

Whether Claims 19-25 are patentable under 35 U.S.C. 103(a) as nonobvious over *Dondeti* in view of *O'Toole.*

VII. GROUPING OF CLAIMS

The claims should not be regarded as all standing together since the claims recite respective limitations that render each claim separately patentable. For this appeal, the following groups are recognized:

A. Independent Claims 1 and 26 and Dependent Claims 3, 4, 9 and 30.

B. Dependent Claim 2.

C. Dependent Claim 5 and 6.

D. Independent Claim 10 and Dependent Claims 8, 11, 12, 15, 16, 18 and 27.

E. Dependent Claims 13, 14 and 28.

F. Independent Claim 19 and Dependent Claims 20, 21, 23 and 25.

G. Dependent Claim 22.

H. Dependent Claim 24.

Claims 17 and 29 are not argued because they are duplicate claims. Applicants offer to cancel claims 17 and 29.

VIII. ARGUMENT

A. None of the Cited Art Teaches an Event Server.

Each of the independent claims recites registration and use of an event server for the purpose of distributing and managing encryption keys for use by network nodes that participate in multicast groups. The record on appeal includes information establishing that an event server is known in the art to provide a distinct set of functionality that does not relate to encryption key management. None of the cited art discloses, teaches, or even remotely suggests an event server.

In the Office Action of November 8, 2002, the Examiner cites *Dondeti* col. 3, line 19-34 to allegedly teach an event server. However, this passage of *Dondeti* does not describe the use of event-based communication. It does not use the term "event server," which has a known meaning in the art. It describes a distributed tree-based key management scheme. In which group control responsibilities and key distribution tasks are delegated to members evenly. This teaches away from Applicants' invention, in which one event server multicasts keys and key changes to all participating group members. The Office Action fails to recognize that an event server is an element having a set of functionality known in the art, but never previously applied to solve the problems that are addressed by Applicants. *Dondeti* fails to teach an event server as that term is understood in the art.

Applicants are the first to conceive of use of an event server for distributing and managing encryption keys for use by network nodes that participate in multicast groups. Therefore, the claims are allowable over the art of record.

B. Independent Claims 1 and 26 and Dependent Claims 3, 4, 9 and 30 are not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claims 1, 26, 3, 4, 9 and 30.

Claims 1, 26, 3, 4, 9 and 30 are directed to an approach for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, and a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes. Each of the subscriber nodes and the publisher nodes receives a unique private key. The approach can determine events that the subscribers and the publishers may process, by the steps of:

> registering the subscribers and the publishers with an **event server** configured to determine whether the publishers are authorized to produce certain events corresponding to event types and whether the subscribers are authorized to receive the certain events in response to the step of registering; and

> generating, with the **event server**, a group session key for establishing the multicast group, the group session key being encrypted in a first message that has a prescribed format.

As stated in MPEP §2143.03: "To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." In Re Royka, 180 USPQ 580. *Dondeti* and *O'Toole*, alone or in combination, fail to disclose, teach or suggest all of the claimed limitations. None of the art of record discloses or in any way renders obvious these limitations.

Dondeti teaches "a distributed tree-based key management scheme." *Dondeti*, col. 3, line 23-24. The system involves a binary distribution tree structure in which group control responsibilities and key distribution tasks are **delegated evenly among group members.**

> Each member is assigned a binary ID and these ID's are used to define key associations for each member. **Members in the key association groups are contacted to report membership changes and to exchange keys.** The members are all trusted equally and all of them may be senders. Prospective members may contact any active member to join the group. **Active members verify new members' credentials and assign them a unique binary ID**... The new member initiates the rekeying process...
>
> Members are represented by the leaves of a binary key distribution tree. **Each member generates a unique secret key for itself and each internal node key is computed as a function of the secret keys of its two children**...
>
> Members of the multicast group are represented by leaf nodes of a key distribution tree. The key distribution tree is strictly binary, i.e. each internal node has exactly two children. **Each member generates a unique secret key** which is the member's contribution towards the generation of the internal nodes keys, including the root key...(col. 3, line 25-col 4, line 2)(emphasis added).

The claims of Group A require "registering the subscribers and the publishers with an **event server**..." and "generating, with the **event server**, a group session key for establishing the multicast group..." Such an event server is not disclosed or in any way suggested by *Dondeti.*

Events are multicasted messages. An event server, as recited in the claims of Group A, establishes secure channels among multicast group members (such as routers in a packet-switched network) and manages group session keys for publishers and subscribers. Publishers and subscribers may register their interest in specific events with the event server, which checks whether a producer is allowed to produce a particular event and whether a subscriber is allowed to receive a particular event. The event server generates and distributes group session keys for establishing multicast groups that use encrypted communications. A publisher sends an event to the event server, which uses a group session key to authenticate and protect the multicast transmission to the event's subscribers. Event servers are not used in any prior approach to establish multicast group keys. No delegation is involved.

Dondeti discusses a tree-based key management system for secure many-to-many group communications, where **members** in key association groups are contacted to report membership changes, exchange keys, verify new members' credentials and assign them a unique ID. *Dondeti* does not disclose or suggest in any way using an **event server** to handle these tasks on behalf of the group members. In fact, in *Dondeti* only **members** are delegated group control responsibilities and key distribution tasks.

The claims of Group A recite, among other features, use of an event server that generates group session keys and distributes these keys to subscribers of an event or message (i.e. to group members). In contrast, each group member in *Dondeti* must independently compute a root key, which is used to encrypt and decrypt multicast data, by using the keys of all nodes in a path to the root as well as the keys of siblings of nodes in a path to the root. *Dondeti*, col. 4, line 11-19; *Dondeti*, col. 9, line 56-57.

Further, an event server as claimed allows a publisher (sender) to target a message only to the event server, which will multicast the message to event subscribers. In contrast, in *Dondeti* a sender must multicast the message itself, *Dondeti*, col. 9, line 57-59, without taking advantage of secure multicast services provided by an event server.

When an event server as claimed updates a group session key (because of normal expiration or group membership changes), the event server creates a new group session key, sends a new message that contains the new group session key to subscribers and notifies the subscribers to reregister. In contrast, in *Dondeti*, when a member leaves, its neighbor initiates the rekeying process. It sends new keys to the members of its key association group, and they are responsible for propagating the new keys to the appropriate members in their subgroups. This teaches away from the claims because **members**, not an **event server**, are said to perform these tasks.

Moreover, *Dondeti* teaches against the methodology of group control that is implemented by an event server: "some form of centralized group control" is stated to be "a common failing" in secure communication systems between many senders and many members under the mistaken belief that all such systems are prone to a single point of failure and are not efficiently scalable. *Dondeti*, col. 1, line 25-28; *Dondeti*, col. 2, line 20-34.

Further, *Dondeti* states that many-to-many secure multicasting calls for decentralized control of the group. "Access control, key distribution and dynamic group management tasks should be delegated to all the senders." (*Dondeti*, col. 1, lines 52-55). Similarly, *Dondeti* states that, with respect to joins and leaves, "undesirable alternative approaches" require one or more entities to keep a snap shot of the key distribution tree, such as when member status report messages are broadcast to a centralized entity that keeps track of all joins and leaves. (*Dondeti*, col. 6, lines 37-42).

With respect to Claim Nos. 1 and 26, the final Office Action asserts that "the step of registering comprises performing an access control check of the subscribers by the event server" is satisfied by the disclosure of *Dondeti* in combination with *O'Toole*. However, O'Toole's disclosure at col. 11 lines 9-34 states:

> Another aspect of the invention features a network-based system for metering of a user's access to linked information that includes a client computer and a server computer interconnected by a computer network. The server computer transmits to the client computer a document containing an embedded link. The client computer activates the embedded link when at least a portion of the of the document corresponding to the embedded link is displayed, records activation of the embedded link in a metering log, and causes information stored in the metering log pertaining to the activation of the embedded link to be transmitted to the server computer.
>
> This process makes it possible to charge a user on a per usage basis for the user's access to information, without requiring the client computer to notify the server computer every time the user accesses the information. The per-usage charges can be assessed even if the client computer stores the documents in a cache from which the client computer periodically retrieves the documents. The information obtained from the metering log may alternatively be used solely for advertising feedback purposes, without any charges to the user.

The cited passage merely describes a technique for transmitting from a server computer to a client computer a document containing an embedded link, activating the embedded link at the client computer and recording activation of the embedded link in a metering log, in order to make "it possible to charge a user on a per-usage basis for the user's access to information, without requiring the client computer to notify the server computer every time the user accesses the information." (O'Toole, col. 3, lines 21-24). This technique in no way involves an access control check, but is instead a means for assessing a user's charges. *O'Toole* does not in any way disclose, teach or suggest an access control check of subscribers by an event server.

Therefore, *Dondeti* taken alone fails to disclose or suggest the limitations of the claims of Group A. *O'Toole* taken alone fails to disclose or suggest the limitations of the claims of Group A. Even taken in combination, assuming that it would have been proper to combine the references, *Dondeti* and *O'Toole* fail to disclose or suggest the limitations of claims in Group A. Thus, the claims in Group A are patentable over *Dondeti* and *O'Toole*, taken individually or in combination.

C. Independent Claim 2 is not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claim 2.

The claim in Group B contains the same limitations as the claims in Group A and in addition further requires at least the following limitations:

> receiving a second message from the subscribers in response to the subscribers updating the group session key; and
> selectively reregistering the subscribers at the event server.

None of the art of record discloses or in any way renders obvious these limitations. In particular, the art of record lacks any disclosure about selectively reregistering subscribers, let alone reregistering them at an event server. Further, since *Dondeti* does not disclose an "event server" as recited in the claims of Group A, *Dondeti* cannot disclose "selectively reregistering the subscribers at the event server."

Therefore, *Dondeti* taken alone fails to disclose or suggest the limitations of the claim of Group B. *O'Toole* taken alone fails to disclose or suggest the limitations of the claim of Group B. Even taken in combination, *Dondeti* and *O'Toole* fail to disclose or suggest the limitations of the claim in Group B. Thus, the claim in Group B is patentable over *Dondeti* and *O'Toole*, taken individually or in combination.

D. Dependent Claims 5 and 6 are not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claims 5 and 6.

The claims in Group C require at least the following limitations:

> wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast group to subscribers with no corresponding objects on the directory.

None of the art of record discloses or in any way renders obvious these limitations.

Claims 5 and 6 require an external authentication service, which is not taught or suggested by the art of record. Instead, *Dondeti* describes a tree-based key management system for secure many-to-many group communications, where members in key association groups are contacted to report membership changes, exchange keys, verify new members' credentials and assign them a unique ID. *Dondeti* does not disclose or suggest in any way using an external authentication service, such as an event server, to handle these tasks on behalf of the group members.

Therefore, *Dondeti* taken alone fails to disclose or suggest the limitations of the claims of Group C. *O'Toole* taken alone fails to disclose or suggest the limitations of the claims of Group C. Even taken in combination, *Dondeti* and *O'Toole* fail to disclose or suggest the limitations of claims in Group C because neither one teaches an external authentication service. Thus, the claims in Group C are patentable over *Dondeti* and *O'Toole*, taken individually or in combination.

E. Independent Claim 10 and Dependent Claims 8, 11, 12, 15, 16, 18 and 27 are not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claims 8, 10, 11, 12, 15, 16, 18 and 27.

The claims in Group D require at least the following limitation:

> modifying an object in the directory based upon the new group session key by using a change password protocol;

None of the art of record discloses or in any way renders obvious this limitation. In particular, the claims of Group D require a "change password protocol", however the art of record does not teach or suggest anything regarding a change password protocol. In *Dondeti*, the "Join Protocol" procedure involves a series of key exchanges among all authorized members, during which the authorized members obtain the keys necessary to compute a new root key, which is used to encrypt and decrypt multicast data. (Dondeti, col. 6, line 21 to col. 7, line 13). In contrast, in the approach of the present invention, key changes involve initiating a key change event from a master event server, and using a change password protocol to generate the new key. As described in the specification at page 19, the key change event includes the new key in an event type object of the key change event, which is multicast to the nodes. Thus, an event server is efficiently used to distribute new keys to nodes participating in a multicast group. This approach is markedly different from *Dondeti* in that it does not use multiple message exchanges and negotiations among members or nodes. Changes are determined at the event server and multicast to participating nodes. The section of *Dondeti* cited in the Office Action thus clearly fails to disclose or suggest the limitation of a change password protocol.

Therefore, *Dondeti* taken alone fails to disclose or suggest the limitations of the claims of Group D. *O'Toole* taken alone fails to disclose or suggest the limitations of the claims of Group D. Even taken in combination, *Dondeti* and *O'Toole* fail to disclose or suggest the limitations of claims in Group D because neither one teaches a change password protocol. Thus, the claims in Group D are patentable over *Dondeti* and *O'Toole*, taken individually or in combination.

Because the art of record fails to disclose or suggest these limitations, the claims in Group D are patentable over the art of record.

F. Dependent Claims 13, 14 and 28 are not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claims 13, 14 and 28.

The claims in Group E require at least the following limitation:

> wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

Claims 13, 14 and 28 require an external authentication service, which is not taught or suggested by the art of record. Instead, *Dondeti* describes a tree-based key management system for secure many-to-many group communications, where members in key association groups are contacted to report membership changes, exchange keys, verify new members' credentials and assign them a unique ID. *Dondeti* does not disclose or suggest in any way using an external authentication service, such as an event server, to handle these tasks on behalf of the group members.

Therefore, *Dondeti* taken alone fails to disclose or suggest the limitations of the claims of Group E. *O'Toole* taken alone fails to disclose or suggest the limitations of the claims of Group E. Even taken in combination, *Dondeti* and *O'Toole* fail to disclose or suggest the claims in Group E because neither one teaches an external authentication service. Thus, the claims in Group E are patentable over *Dondeti* and *O'Toole*, taken individually or in combination.

Because the art of record fails to disclose or suggest these limitations, the claims in Group E are patentable over the art of record.

G. Independent Claim 19 and Dependent Claims 20, 21, 23 and 25 are not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claims 19, 20, 21, 25 and 25.

The claims in Group F require at least the following limitation:

> one or more processors coupled to the bus for selectively generating a group session key and private keys corresponding to the plurality of nodes, the group session key being updated by utilizing a change password protocol to modify an object corresponding to the events in the directory.

The claims of Group F require a "change password protocol." As described above with respect to the claims of Group D, the art of record does not teach or suggest anything about a change password protocol. The claims of Group F are patentable over *Dondeti* and *O'Toole*, taken individually or in combination, for the same reasons stated above with respect to Group D.

O'Toole, taken individually or in combination, for the same reasons stated above with respect to Group D.

H. Dependent Claim 22 is not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claim 22.

The claim in Group G requires at least the following limitation:

> … the directory authenticates by using authentication services of the directory in conjunction with Kerberos service that allows extending membership to the multicast groups to nodes with no objects in the directory.

None of the art of record discloses or in any way renders obvious this limitation. Indeed, the Office Action does not cite any passage of the cited art to show this limitation. This is not surprising, because neither *Dondeti* nor *O'Toole* involve interoperation with the Kerberos service. The references also do not address how to extend membership to nodes that do not have corresponding objects in a directory; the authors of *Dondeti* and *O'Toole* apparently did not anticipate this problem. Because the art of record fails to disclose or suggest this limitation, the claims in Group G and the claims dependent thereon are patentable over the art of record.

I. Dependent Claim 24 is not rendered obvious by *Dondeti* in view of *O'Toole* because neither *Dondeti* nor *O'Toole*, taken alone or in combination, disclose, teach or suggest all the limitations that are required by Claim 24.

The claim in Group H requires at least the following limitation:

> modifying the object based upon the new group session key by using a change password protocol.

None of the art of record discloses or in any way renders obvious this limitation.

O'Toole, taken individually or in combination, for the same reasons stated above with respect to Group D.

IX. CONCLUSION AND PRAYER FOR RELIEF

The rejections of the final Office Action under 35 U.S.C. § 103 lack the requisite factual and legal basis. The applied references, *Dondeti* and *O'Toole*, do not disclose or suggest the numerous features of the rejected claims for the specific reasons discussed above. Appellants therefore respectfully submit that the rejections under 35 U.S.C. § 103 are incorrect and respectfully solicit the Board to **reverse** each of the imposed rejections under 35 U.S.C. § 103, and to remand the case to the Examiner for further proceedings.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

By: ______________________
Christopher J. Palermo
Attorneys for Applicants/Appellants

1600 Willow Street
San Jose, CA 95125
(408) 414-1213
Date: February 6, 2003
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box AF, Commissioner for Patents, Washington, D.C. 20231

on 2/6/03 by

APPENDIX

1. A method for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes, wherein each of the subscriber nodes and the publisher nodes receives a unique private key and that can determine events that the subscribers and the publishers may process, the method comprising the steps of:

registering the subscribers and the publishers with an event server configured to determine whether the publishers are authorized to produce certain events corresponding to event types and whether the subscribers are authorized to receive the certain events in response to the step of registering; and

generating, with the event server, a group session key for establishing the multicast group, the group session key being encrypted in a first message that has a prescribed format.

2. The method as recited in Claim 1, further comprising the steps of:

receiving a second message from the subscribers in response to the subscribers

determining whether the first message corresponds to a correct key version;

updating the group session key; and

selectively reregistering the subscribers at the event server.

3. The method as recited in Claim l, wherein the prescribed format of the first message conforms with lightweight directory access protocol (LDAP).

4. The method as recited in Claim 1, wherein the prescribed format of the first message comprises a protocol version number field, a message type field, and a message length field.

5. The method as recited in Claim 1, wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast group to subscribers with no corresponding objects in the directory.

6. The method as recited in Claim 5, wherein the external authentication service is supplied by a Kerberos server.

7. The method as recited in Claim 1, wherein the event server manages the private keys of the subscribers and the publishers.

8. The method as recited in Claim 2, wherein the step of updating comprises:
creating a new group session key;
modifying an object in the directory based upon the new group session key by using a change password protocol;
sending a new message that contains the new group session key to the subscribers; and
notifying the subscribers to reregister.

9. The method as recited in Claim 1, wherein the step of registering comprises performing access control check of the subscribers by the event server.

10. A communication system for creating a plurality of secure multicast groups in a network that includes a plurality of principals configured for functioning as subscribers and publishers, each of the principals having a private key, a multi-master directory comprising a directory server for communicating with one or more of the principals to authenticate each of the principals and to provide access control, the multi-master directory controlling access on a per object and per attribute basis, the communication system comprising:

an event server coupled to the plurality of principals for registering the plurality of principals and for determining whether the principals are authorized to produce certain events when the principals are functioning as publishers and whether the principals are authorized to receive the certain events when the principals are functioning as subscribers; and

means in the event server for creating a group session key for establishing one of the multicast groups, by distributing the group session key in an encrypted message to the subscribers, the encrypted message encapsulating the group session key according to a prescribed format;

means in the event server for updating the group session key by utilizing a change password protocol to modify an object in the directory;

means in the event server for notifying the subscribers to reregister in response to the updating of the group session key.

11. The communication system as recited in Claim 10, wherein the directory server is collocated with the event server, the directory server and the event server participating in a common one of the multicast groups.

12. The communication system as recited in Claim 10, wherein the prescribed format of the message conforms with lightweight directory access protocol (LDAP).

13. The communication system as recited in Claim 10, wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

14. The communication system as recited in Claim 13, wherein the external authentication service is supplied by a Kerberos server.

15. The communication system as recited in Claim 10, wherein the prescribed format of the message comprises a protocol version number field, a message type field, and a message length field.

16. The communication system as recited in Claim 10, wherein the event server manages the private keys.

17. The communication system as recited in Claim 10, wherein the event server updates the group session key by performing the steps of:

creating a new group session key;

modifying the object based upon the new group session key by using the change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

18. The communication system as recited in Claim 10, wherein the event server performs access control check of the subscribers during registration of the subscribers.

19. A computer system functioning as an event server and for establishing multiple secure multicast groups, the computer system comprising:

a communication interface for communicating with a plurality of nodes and for interfacing a multi-master directory to authenticate the computer system and the plurality of nodes, the multi-master directory having access controls on a per object and per attribute basis, wherein the nodes access the directory to determine events that the nodes may process;

a bus coupled to the communication interface for transferring data;

one or more processors coupled to the bus for selectively generating a group session key and private keys corresponding to the plurality of nodes, the group session key being updated by utilizing a change password protocol to modify an object corresponding to the events in the directory;

an event server that is executed by the one or more processors; and

a memory coupled to the one or more processors via the bus, the memory including one or more sequences of instructions which when executed by the one or more processors cause the one or more processors to perform the steps of registering the plurality of nodes, determining whether the nodes are authorized to produce and authorized to receive certain events corresponding to objects of the directory, distributing the group session key to the nodes via a message, the message encapsulating the group session key according to a prescribed format, and selectively reregistering the nodes in response to updating the group session key.

20. The computer system as recited in Claim 19, wherein the directory is collocated with the event server, the directory and the event server participating in a common one of the multicast groups.

21. The computer system as recited in Claim 19, wherein the prescribed format of the message conforms with light weight directory access protocol (LDAP).

22. The computer system as recited in Claim 19, wherein the directory authenticates by using authentication services of the directory in conjunction with a Kerberos service

that allows extending membership to the multicast groups to nodes with no objects in the directory.

23. The computer system as recited in Claim 19, wherein the event server manages the private keys of the plurality of nodes.

24. The computer system as recited in Claim 19, wherein the event server updates the group session key by performing the steps of:

creating a new group session key;

modifying the object based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

25. The computer system as recited in Claim 19, wherein the computer system performs access control check of the nodes during registration.

26. A computer-readable medium carrying one or more sequences of instructions for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes, whereby each of the subscriber nodes and the publisher nodes receives a unique private key and that

can determine events that the subscribers and the publishers may process, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

registering the subscribers and the publishers with an event server, the event server determining whether the publishers are authorized to produce certain events corresponding to event types and whether the subscribers are authorized to receive the certain events in response to the step of registering; and

generating a group session key for establishing the multicast group, the group session key being encrypted in a first message that has a prescribed format.

27. A computer-readable medium as recited in Claim 26, further comprising the steps of:

receiving a second message from the subscribers in response to the subscribers

determining whether the first message corresponds to a correct key version;

updating the group session key; and

selectively reregistering the subscribers at the event server.

28. A computer-readable medium as recited in Claim 26, wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

29. A computer-readable medium as recited in Claim 27, wherein the step of updating comprises:

creating a new group session key;

modifying an object in the directory based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

30. A computer-readable medium as recited in Claim 26, wherein the step of registering comprises performing access control check of the subscribers by the event server.